Certification Practice Statement

Certificate Policy

REGIONE DEL VENETO

AZIENDA ZERO

General information

Documentary control

Security classification:	Public
Target entity:	AZIENDA ZERO
Version:	2.1
Edition date:	23.03.2020
File:	CPS_v.2.1_EN

Formal state

Written by:	Approved by:
Name: UOC Sistemi Informativi – IT Department Date: 23.03.2020	Name: UOC Sistemi Informativi – Management Department Date: 25.03.2020

Versions control

Version	Chages	Description of change	Date
1	Original	First version of the document	14.01.2019
1.1	Detailed identification of the various parties involved in the outsourcing service Section. 8.4 – Considerations about service accessibility	Second version of the document	15.02.2019

1.1 rev. 1	External links. “Approved by” section.	Revision	27.02.2019
2.0	New version of the document	New version	15.01.2020
2.1	Par. 9.1.1. Update - Annex A – Qualified electronic certificate verification system (new)	Review and update	23.03.2020

Index

1. Introduction

1.1. Presentation

This public document, also called "*Certification Practice Statement*" (CPS) describes the operative procedures followed by AZIENDA ZERO for the provision of the following Trust Services:

- Issuance of qualified signature certificates;
- Issuance of qualified time stamp certificates;
- Time stamp generation.

The certificates issued according to this CPS are the following:

- **Qualified certificate of subscription**
  - Qualified certificate of subscription on remote QSCD
- **Time Stamping Unit Certificate**
  - Certificate of Time Stamping Unit for the issue of qualified time stamps.

The Qualified Trust Services provided by AZIENDA ZERO meet the requirements of EU Regulation No.910/2014 (eIDAS) and comply with the following standards:

• ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

• ETSI EN 319 411 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing certificates.

• ETSI EN 319 412 Electronic Signatures and Infrastructures (ESI); Certificate Profiles.

• ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.

• ETSI EN 319 422 Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles.

The structure of this CPS is based on the RFC 3647 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" public specification.

1.2. Document name and identification

This document is the "Certification Practice Statement / CPS" of AZIENDA ZERO.

The current version of this manual is indicated in the document header and in the "Versions control" section.

OID (Object Identifier)

The OID (Object Identifier) of the policies supported by this Certification Practice Statement are listed below. AZIENDA ZERO has assigned an object identifier (OID) to each certificate policy, for their identification by requests.

OID	Type of certificates
	Electronic signature service
1.3.6.1.4.1.52658.1.1.1	Qualified certificate of subscription on remote QSCD
	Time Stamping service
1.3.6.1.4.1.52658.1.2.1	*Time Stamping Unit Certificate*

In case of contradiction between this Certification Practice Statement and other documents of supply conditions and / or procedures relating to the services offered by AZIENDA ZERO, the established in this Practice Statement will prevail.
Azienda Zero reserves the right to make changes to this Practice Statement for technical needs or procedural changes that occurred during the service management.
When any change occurs, Azienda Zero will notify AGID of the updated version of the Practice Statement that will be published on its institutional websites. This document is published on the AZIENDA ZERO website https://www.azero.veneto.it/.

1.3. Participants in the certification services

1.3.1. Qualified Trust Service Provider - TSP

AZIENDA ZERO through the collaboration of technological experts Bit4id S.r.l. and Uanataca S.A., operates as a Qualified Trust Service Provider (QTSP).The Organization identifying data are as follows:

AZIENDA ZERO REGISTERED OFFICE: PASSAGGIO LUIGI GAUDENZIO, 1 - 35131 PADOVA

TELEPHONE: 049/8778178, 049/8778236, 049/8778249
EMAIL: SUPPORTO.CA@AZERO.VENETO.IT

AZIENDA ZERO provides the following trust services:

- Release of qualified certificates, in compliance with the provisions of Regulation (EU) no. 910/2014 (briefly referred to as the "eIDAS Regulation") and the "ETSI" technical standard applicable to the issue and management of qualified certificates, with particular reference to the standard "EN 319 411-1" and "EN 319 411-2".
- Release of qualified time stamps in compliance with the provisions of Regulation (EU) no. 910/2014 (briefly referred to as "eIDAS Regulation") and to the "ETSI" technical standard applicable to the issue and management of qualified certificates, with particular reference to the "EN 319 421" standard.

To provide qualified trusted services, AZIENDA ZERO uses several certification keys.

1.3.1.1. Azienda Zero CA Qualified eIDAS 1

This is the CA that issues certificates to the end-user and whose public key certificate has been self-signed.

Identification data:

CN:	Azienda Zero CA Qualificata eIDAS 1
Fingeprint:	fb6b79978e7d9062322acbe431d24cc92c278001
Valid from:	11th January 2019
Valid until:	11th January 2044
RSA key length:	4.096 bits

1.3.1.2. AZIENDA ZERO CA2 2016

This is the CA that issues certificates for the issue of time stamp and whose public key certificate has been self-signed.

Identification data:

CN:	Azienda Zero TSA Qualified elDAS 1
Fingeprint:	97217b8d2bccd5cacb6dbe61619c421412dbf266
Valid from:	11th January 2019
Valid until:	11th January 2044
RSA key length:	4.096 bits

1.3.2. Registration Authorities - R.A.

The Registration Authorities (R.A.) constitute third parties delegated by AZIENDA ZERO, that, through the stipulation of special agreements, are delegated to carry out the identification and authentication activities of the subjects requesting the certificates.
The R.A. performs the following tasks:

- Identification and Authentication (I&A) of the subject requesting signing certificate;
- Verification of the conditions required to meet the applicant certificate request;
- Verification of the identification data of the person who will be the certificate owner;
- Applicants (future owners) and corresponding data registration;
- Authorization for the issuance of digital certificates through dedicated tools made available by Azienda Zero;
- Storage of the documentation related to the a) identification of subscribers; b) registry of the subrscribers; c) management of the life cycle of the certificates.

They will be able to act as RA of AZIENDA ZERO:

- Any natural or legal person external to the company authorised by AZIENDA ZERO;
- AZIENDA ZERO directly, through his staff.

AZIENDA ZERO contractually will formalise the reations between itself and each of the entities that act as Registration Authority.

The R.A., will be able to authorise one or more persons to act as Trader of the RA: This one willb be able to delegate the identification functions of the subscribers (or futur owners), prior agreement for the delegation of these functions.
AZIENDA ZERO will need to expressly authorise the collaboration agreement.
R.A. are only activated following a proper training of the staff employed.

R.A. are also subject to periodic audits by AZIENDA ZERO with the aim of verifying compliance with the agreements signed with the CA and the procedures defined in this document.

1.3.3. End entities

The end entities are the natural persons receiving the services of the isssuance, management and use of digital certificates issued by AZIENDA ZERO.

The end entities of AZIENDA ZERO of certification services will be the following:

1. Subscribers: natural persons who request the CA to issue a digital certificate;
2. Signers: natural persons holding the qualified certificate, coincide with the Subcribers following the issue of the certificate;
3. Relying parties: subjects who receive an electronic document signed with the digital certificate of the Signer and who rely on the validity of the certificate itself (and / or on the digital signature therein) to assess the correctness and validity of the document itself, in the contexts where it is used;

1.3.3.1. Subscribers of the certification

It is the natural person that requires the issuance of digital certificates, addressing directly to the CA or to an RA.
The subscriber is therefore, the “Client” of the CA: at the time of the formal request for a certificate, declares to accept the General Conditions of contract established by the CA and consent to the exercise of rights and obligations.
The contractual conditions od the CA are additional and do not prejudice the rights and obligations of the Subscribers and/or Signers regulated in the European technical standards applicable to the issuance of qualified electronic certificates, specially “ETSI EN 319 411”, sections 5.4.2 e 6.3.4.e.
Following the issuing of the certificate, the Subcriber identity himself with the Signer.

1.3.3.2. Signers of the certificate

The Signer is the person who owns and uses the private key related to an electronic certificate.

The Signer is identified within the certificate through a Distinguished Name (DN), in the Subject field, complying with the ITU-T X.500 standard.
In the Subject field the identifyng details of the Signers of the certificate are inserted, without being possible, in general, the use of pseudonyms.
The private key of a signer cannot be recovered or deducted by the CA, so the natural persons identified in the relevant certificates are the sole responsible for their protection and should consider th implications of losing a private key.

1.3.3.3. Relying parties (R.P.)

The Relying Parties are the persons and organisations who rely on the information contained in the certificates issued by AZIENDA ZERO.
In particular, for the service described in this Certification Practice Statement, for R.P. we mean all the subjectes that verify the electronic signatures and the electronic seals throught the certificates issued according to this Certification Practice Statement.
All the persons who must rely on the information contained in the certificates have the obligation, before accepting a certificate, to carry out the necessary checks, according to the provisions in this Certification Practice Statement or the instructions available on the AZIENDA ZERO.

1.3.4. Outsourcee

AZIENDA ZERO offers the service of certification of public keys using the technological partnership of

- Bit4id Srl, a company founded in 2004 with proven experience in the field of public key infrastructure (PKI technology) and with numerous successful experiences in the Italian and international field ;
- Uanataca S.A., QTSP founded in 2015 and with its registered office in Barcelona (Spain).

These companies are responsible for the technical management of technical and logistic systems and services, outsourced.
In particular, it is entrusted with the outsourcing of certain CA services with particular reference to:
- Definition of security objectives;

- Identification of contractual and regulatory requirements;
- Risk assessment for the analysis, evaluation, planning of risk treatment and selection of relevant countermeasures.

By outsourcing the services provided by the CA to qualified Suppliers, Aziendo Zero intends to guarantee the confidentiality, integrity and availability of information.

1.3.5. Authority

1.3.5.1. Agenzia per l'Italia Digitale "Agency for Digital Italy" – AgID

The Agenzia per l'Italia Digitale (AgID) is the body that, pursuant to Article 17 of the eIDAS Regulation, carries out supervisory activities on the Providers of qualified trust services established in the Italian territory in order to ensure compliance with the requirements established by the Regulations.

1.3.5.2. Conformity Assessment Body

The conformity assessment body (CAB, acronym for Conformity Assessment Body) is an accredited body, as required by the eIDAS Regulation, responsible for assessing the compliance of the Qualified Trust Service Provider and the qualified trust services provided by it. regulations and applicable standards.

1.4. Use of certificates

This section lists the requests for which each type of certificate can be issued by AZIENDA ZERO, sets limitations to certain requests and prohibits certain requests of certificates.

1.4.1. Uses permitted for certificates

The certificates issued by AZIENDA ZERO, according to the methods indicated in this Certification Practice Statement, are Qualified Certificates under the CAD and the eIDAS rules. The certificate issued by the CA will be used to verify the qualified signature of the owner to whom the certificate belongs.
Other uses of certificates are not foreseen and are to be avoided. In particular, it is forbidden to use the certificate outside the limits and contexts specified in the Operational Manual, in the contractual documentation and in violation of the limits of use and value (key usage, extended key usage, user notice) indicated in the certificate.
AZIENDA ZERO reserves the right to revoke the certificates if it becomes aware that these certificates have been used improperly.

1.4.1.1. Qualified Certificate of subscription on remote QSCD

This certificate has the OID 1.3.6.1.4.1.52658.1.1.1. It is a qualified certificate in accordance with Article 28 of the Regulation EU 910/2014 eIDAS, which is issued in QSCD for the electronic signature and authentication, in accordance to the certification statement QCP-n-qscd with the OID 0.4.0.194112.1.2.

It works with qualified signature creation devices (QSCD), as referred to Articles 29 and 51 of the Regulation (EU) 910/2014, according to the technical regulation issued by the European Telecommunications Stadards Institute, identified with the reference EN 319 411-2.

It guarantee the identity of the Signer and it allows the generation of a “qualified electronic signature”, that is an advanced electronic signature based on a qualified certificate, and generated using a qualified device, which is equivalent, for all legal purposes, to a written signature without the need for additional requirements.

In addition the certificate can be used for applications that do not require an electronic signature equivalent to the written signature, such as:

a) Signature of secure e-mail;

b) Other digital signature applications.

The “key usage” allows to perform the functions of “Content commitment”.

1.4.1.2. Qualified certificate of Time Stamping Unit

This certificate has the OID 1.3.6.1.4.1.52658.1.2.1 and it si issued in accordance with the certification statement QCP-l-qscd with the OID 0.4.0.194112.1.3.
The certificates of Time Stamping Unit are generated for the issue of timestamps..

The synchronisation of the times in Azienda Zero is done with a timeserver NTP Stratum 3.

1.4.2. Limits and forbidden uses of certificates

Certificates issued by AZIENDA ZERO are used for their own function and the established purpose of this Certification Practice Statement, not being able to be used for other functions or other purpose and in violation of the limits of use and value (key usage, extended key usage, user notice) listed within the certificate itself.

Likewise, certificates issued by AZIENDA ZERO must be used only in accordance with the applicable law.

1.5. Administration of the Certification Practice Statement

1.5.1. Organisation that administers the document

This document is the CPS of AZIENDA ZERO and is written, published and updated by AZIENDA ZERO.
Contact information of the TSP are the following:
Azienda Zero
Passaggio Luigi Gaudenzio, 1 - 35131 Padova (PD)
Padova (Italia)
protocollo.azero@pecveneto.it

Codice Fiscale 05018720283

https://azero.veneto.it/ca

1.5.2. Approval and management procedure

AZIENDA ZERO, with the support of the Outsourcee, performs a conformity check of this Certification Practice Statement to the certification service delivery process and to the conditions associated with it.

This document is reviewed (and updated, if necessary) at least annually.

1.6. Definitions and acronyms

CA: Certification Authority

CAB: Conformity Assessment Body

CAD: Codice dell'Amministrazione Digitale (D.lgs. n.82/2005)

CP: Certificate Policy

CRL: Certificate Revocation List

CSP: Certification Practice Statement

ETSI: European Telecommunications Standards Institute

FQDN: Fully-Qualified Domain Name

HSM: Hardware Security Module

HTTP: Hyper-Text Transfer Protocol

I&A: Identification and Authorization

RO: Registration Officer

OCSP: On-line Certificate Status Protocol

OID: Object IDentifier

PKI: Public Key Infrastructure

QSCD: Qualified Signature-Creation Device

RA: Registration Authority

TLS: Transport Layer Security

TSL: Trust-service Status List

TSP: Trust Service Provider

2. Publication of certificates information and Repository

2.1. Repository

AZIENDA ZERO has an on-line Deposit of certificates (c.d. repository), in which the information related to the certification services is published.
This "repository" is published at the link https://azero.veneto.it/ca/
The "repository" is available 24 hours (7x24).
In case of the system failure was beyond the AZIENDA ZERO control, it will ensure that the service is back available within the prescribed time in the section 5 of this certification practice statement.

2.2. List of the information published by the CA

AZIENDA ZERO publishes on its website:

- The revoked certificates list (RCL);
- The PKI Disclosure Statements (PDS);
- The Certification Practice Statement (CPS)
- The general Terms and Conditions;
- The Trust Services Forms;
- The PKI certificates.

2.3. Frequency of publication

The information of the CA, including this Certification Practice Statement and the related documentation is published when available.

Changes to the Certification Practice Statement are subject to the provisions of section 1 of this document.

The information of the revocation status of the certificates will be published in accordance with the established in the section 4 of this Certification Practice Statement.

2.4. Access control

AZIENDA ZERO does not limit the read access to the information established in the section 2, but establishes controls to prevent non-authorised people to add, modify or delete these information, to protect their integrity and authenticity.

3. Identification and authentication

3.1. Names

3.1.1. Type of names

All certificates contain a distinguished name (DN), compliant with the standard X.501, in the field *Subject*, including a *Common Name* (CN=), relative to the identity of the Subscriber, as well as several additional informationin the field *SubjectAlternativeName*.
The DN attributes enhancement rules comply with ETSI EN policies in relation to the certificates profiles of natural persons and the specifications included in RFC 5280.
In particular, certificates issued according to this CPS are compliant with the following standards:

- ETSI EN 319 411-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
- ETSI EN 319 411-2: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.
- ETSI EN 319 412-1: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures.
- ETSI EN 319 412-2: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons.
- ETSI EN 319 412-5: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements.

3.1.2. Meaning of names

The names on the certificates are as follows:

- Country
- Organization
- Organization Unit
- Organization Identifier
- Title
- Surname

- Given Name
- Serial Number
- Common Name

The names in the fields of the certificates *SubjectName* and *SubjectAlternativeName* are understandable in natural language and will have to be significant in order to enable the correct identification of the certificates subjects and the Time Stamp Unit certificates.

3.1.2.1. Issuance of certificates of the set of tests

In case the provided data in the *DN* or *Subject* were fictitious (e.g "Test Organisation, "Test First Name", "Surmane test") or expressly stated words indicating its invalidity (e,g. "TEST", "EVIDENCE" or "INVALID"), the certificate will be considered as legally invalid and therefore with no responsibility for AZIENDA ZERO.
These certificates are issued to take interoperability tests and allow the regulatory body its assessment.

3.1.3. Use of anonymous and pseudonymous

Under no circumstances can the pseudonymous be used for identifying a Signer. Likewise, under no circumstances can anonymous certificates be issued.

3.1.4. Interpretation of name formats

For the rules of interpretation of names, the ITU-T standard relating to directory services (ITU-T X.500 or ISO / IEC 9594) is respected.

3.1.5. Uniqueness of names

To ensure the unambiguous correlation between the owner and the certificate, the subject section of the latter can never be identical for two distinct owners. Therefore, as indicated in the ETSI EN 319 412 standard regarding the certificate issuance profiles, the Subject field (SubjectDistinguishedName) contains specific identification attributes based on the nature of the Owner.
In particular, uniqueness is guaranteed by the following attributes:
• the Serial Number (OID 2.5.4.44) containing the tax code of the subject or, alternatively, an identification code in compliance with ETSI EN 319 412-1 (such as the passport or identity card number of the owner)

• the Given name (OID 2.5.4.44) containing the name of the subject

•the Surname (OID 2.5.4.44) containing the subject's surname

Uniqueness for TSU certificates is also ensured by AZIENDA ZERO procedures.

3.1.6. Resolution of name conflicts

AZIENDA ZERO won't be required to first determine that an subscriber of certificates has industrial property rights on the name of a certificate request, but at first will proceed to certify it.

Futhermore, it won't act as arbitror or mediator, or in any other way to resolve any dispute concerning the property of names of persons or organisations, web domains, brands or commercial names.

However, in case of AZIENDA ZERO receives a notification concerning a name conflict, according to the legislation of the subscriber's country, it may take appropriate actions to block or withdraw the certificate issued.

In any case, the CA reserves the right to reject the certification request due to names conflict.

3.2. Initial identity validation

The CA. verifies with certainty the identity of each Subscriber at the first request for the issue of a qualified certificate in order to ensure that that certificate can accurately and completely refer to the Subscriber; therefore, before proceeding with the issue of the required certificate, the C.A. must carry out all the necessary activities for the identification of the Subscribers.

The identity of the Subscriber for the certificate is verified through his identity document

as well as through specific attributes that can be: the association with the organization to which it belongs and, possibly, the role held within the organization.

The identification operation is carried out in compliance with the provisions of current legislation: the person in charge of carrying out the identification activities will therefore be required to verify the identity of the subscriber by checking with one of the documents having legal validity pursuant to 'art. 35 d.P.R. of December 28, 2000 n. 445 of which are included (Identity card, Passport, Driving license, License to drive pleasure craft, Pension booklet, License to run thermal plants, Firearms license).

All the documentation thus acquired and verified will be kept by the CA, in accordance with the provisions of Regulation (EU) 2016/279 - GDPR - of the European Parliament

and of the Council of 27 April 2016 and subsequent amendments, for as long as necessary to ensure use. and the continuity of the service requested.
To guarantee the protection and management of personal data acquired during the registration procedures, moreover, privacy information will be provided in advance to each subcribert.
For details of the identification procedure of a natural person, it is possible to refer to par. 3.2.2. below.

3.2.1. Proof of possession of the private key

The possession of the private key is demonstrated under the reliable process of delivery and acceptance of the certificate by the Subscriber and/or by the Signer.

3.2.2. Authentification of natural person identity

This section describes the testing methods of the identity of a natural person identify in the certificate.
The operators responsible for verifying the identity of the natural persons requesting the Certificate carry out the identification operations according to the methods provided in this Operating Manual, in compliance with the guidelines set out in Pr. 6.2 of ETSI EN 319 411-2 and subsequent amendments and the criteria set out in the "Baseline Requirements Guidelines" and clause 11 of the "Extended Validation Certificate Guidelines".

3.2.2.1. In the certificates

The identity of the natural persons who sign identified in the certificates is validated through a production of its official document od identification (Identity card, Passport, Driving license, License to drive recreation craft, Retirement booklet, Heating system license, Firearms license or any other identification number recognised by law).

3.2.2.2. Identity validation

The identification procedure involves the physical presence of the Subscriber, at least 18 (eighteen) years of age, in front of an Operator or personnel authorized by R.A. of AZIENDA ZERO, who verify the identity of the Subscriber by verifying the corresponding identity documents shown in the original.
It is necessary that the Subscriber is in possession of the Fiscal Code (Health Card, Fiscal

Code Card, Certificate of attribution of Fiscal Code, etc.) whose performance can be requested by the subjects authorized to perform the recognition; failing this, it will be possible to use a similar identification code (e.g. social security code) or the passport identification number.
In the case of a natural person, in fact, the staff in charge of the verification will ascertain the following types of data:
- Fullname (first name, name and surname);
- Date and place of birth;
- Address of residence and domicile;
- Fiscal Code;
- E-mail address or p.e.c .;
- Type and number of the identity document presented;
- Authority that issued the document, date and place of issue, expiry date;
- any other data deemed useful for identification purposes;

In the event that the subject to be identified is a natural person identified in association with a legal person (of which he is dependent or linked by a collaborative relationship), the employee will acquire the following information:
- Full name (first name, name and surname);
- date and place of birth;
- residence and domicile address;
- Fiscal Code;
- E-mail address or p.e.c .;
- Type and number of the identity document presented;
- Authority that issued the document, date and place of issue, expiry date;
- full name and company name of the associated legal person;
- any existing registration information relating to the associated legal person;
- type of affiliation of the natural person to the legal person and documentation proving this relationship.
- any other data deemed useful for identification purposes;

This process allows a rigorous verification and verification of the identity of the natural person in the certificate. For this reason, in all cases where a certificate is issued, the identity of the natural person is always previously validated by an authorized Registration Operator.
It will be the responsibility of the Subscriber to provide, at the end of the physical identification operations, to provide a physical or home address where the latter can always be contacted.
The Registration Office will verify, by viewing documents or through its own sources of information, the rest of the data and attributes to be included in the certificate, keeping the documentation that proves its validity.
The identification procedure can also be carried out by a Public Official on the basis of

the provisions of the regulations governing their activity, including the provisions of Legislative Decree May 3, 1991, n. 143 and as amended
Once the identification procedure has been completed by an authorized Operator, the latter is required to collect and archive the originals of all the documentation relating to each individual request for the issue of the Certificates as well as all the documentation relating to the identification of the Subscribers which will be communicated in advance to Azienda Zero, also in electronic format, in order to correctly activate the Certificate issuance procedure.

3.2.3. Not verified information

AZIENDA ZERO does not include any information of the Subscriber and/or the Signer not verified in the certificates.

3.2.4. Authentication of the identity of a RA and its operators

For the construction of a new Registration Authority (RA) AZIENDA ZERO performs the necessary checks in order to confirm the existence of the identity or organisation involved. For that purpose, AZIENDA ZERO will ne able to use the production of documents or use its own information sources.

Likewise, AZIENDA ZERO, directly or through its Registration Authority, verifies and validates the operator's identity of the Registration Authorities, and they send AZIENDA ZERO the relevant identification documentation of the new operator, together with its authorisation to act in such capacity.

AZIENDA ZERO is assured that the operators of the Registration Authority receive the proper training for the performance of their duties, which is verified with a relevant assessment. The RA previously approved by AZIENDA ZERO can execute such training and assessment.

For the delivery of services, AZIENDA ZERO ensures that the operators of the Registration Authority have access to the system via strong authentification with digital certificate.

3.3. Identification and authentication of renewal requests

3.3.1. Identification and authentication for certificates routine renewal

The identification and authentication procedure, in cases of renewal of qualified certificates, is simpler than that relating to the first issue request.

Before renewing a certificate, the operator or the authorised personnel of AZIENDA ZERO's Registration Authority verifies that the information used to the the identification of the Subscriber and / or the Owner continue to be valid and have no undergone changes.

The acceptable methods for such verifications are:

• The use of the Reserved emergency code ("user code") related to the previous certificate, or other methods of personal authentification, that consist in information that only the natural person identified in the certificate knows, and allows in an automatic way the renewal of the certificate, as long as the deadline legally established hasn't exceed;

• The use of the current certificate for its renewal as long as it has not exceeded the deadline legally established for this possibility.

If any information of the Subscriber or Signer identified in the certificate has changed, the new information must be properly registered so a complete authentication is done, in accordance with the established in the section 3.

3.3.2. Identification and authorisation for renewal requests after revocation

In the event that a renewal of the certificate is required after its revocation, it is necessary for the Applicant to repeat the identity validation procedure referred to in par. 3.2.2.2.

Before generating a certificate to a subscriber whose certificate was revoked, the operator or the authorised personnel of AZIENDA ZERO's R.A. will verify that the information used that day to verify the identity and the rest of the data of the Subscriber and the Signer are still valid, in which case previous section shall apply.

The renewal of the certificates after their revocation will not be possible in the following cases:

• the certificate was revoked by erroneous issuance to a person different that the one identified in the certificate;

• the certificate was revoked by a non-authorised issuance of the person identified in the certificate;

• the certificate revoked may contain misleading or fake information.

If any information of the Subscriber (or the Signer) identified in the certificate has changed, the new information must be properly registered so a complete authentication is done, in accordance with the established in the section 3.

3.4. Identification and authentication of revocation

AZIENDA ZERO or authorised personnel of the R.A., manage the requests relative to revocation of a certificate.

The identification of the Subscribers and/or Signers during the process of revocation of the certificates can be performed by:

• The Subscriber and/or Signer:
  - Through the ERC via AZIENDA ZERO's web page (https://azero.veneto.it/ca) in 24/7 schedule;
  - Other media, as telephone, e-mail, etc. when there is a reasonable assurance of the identity of the applicant for revocation in the judhement of AZIENDA ZERO and/or R.A.

• The R.A.: they must identify the Signer before approving a revocation request using the methods they consider appropriate.
When the Subscriber would want to initiate a revocation request, and there were doubts for its identification, during office hours, his certificate would go onto suspensions status.

4. Certificate life-cycle operational requirements

4.1. Certificate issuance request

4.1.1. Legitimation to apply for the issuance

The Applicant of the certificate must sign the contractual documentation drown up by AZIENDA ZERO.

4.1.2. Procedures and responsabilities

AZIENDA ZERO receives certificates request : the requests are implemented by a document in paper or electronic format, individually or in batches, through external databases or interface of Web Services whose addresse is AZIENDA ZERO.

The request will go together with the supporting documentation of the identity and other circumstances of the natural person identified in the certificate, in accordance with the established in the section 3. Also, an adress or other data that will allow contacting the natural person identified in the certificate.

4.2. Processing the certification request

4.2.1. Implementation of identification and authentification functions

Once received the request of a qualified certificate issuance, AZIENDA ZERO ensures that the request is completed, precise and duly authorised, before processing it.

If so, AZIENDA ZERO verifies the information provided, verifying the aspects described in section 3.

In case of qualified certificate, the supporting documentation of the approval of the request must be preserved and properly registered with guarantees of security and integrity during 20 years from the expiration of the certificate, even in case of early loss effective for renovation.

4.2.2. Approval or rejection of the request

In case the data is correctly verified, AZIENDA ZERO should approve the request of the certificate and proceed with its issuance and delivery.

If the verification indicates that the information is non correct or such information is deemed unreliable, inaccurate, incomplete or inconsistent, AZIENDA ZERO will deny the request, or will stop its approval up to having made the additional checks that it considers appropriate.

AZIENDA ZERO will definitely deny the request in case the additional checks won't help to correct the information to verify.

AZIENDA ZERO will notifie tha approval or denial of the request to the applicant.

AZIENDA ZERO will be able to automate the verification procedures of the information correction that will be in the certificates, and the approval of the requests.

4.2.3. Time to process certificate requests

AZIENDA ZERO elabora le richieste di certificati in ordine di arrivo, entro un termine di tempo ragionevole.
Requests remain active until its approval or rejection.

4.3. Certificate issuance

4.3.1. Issuance process

After approving the certification request, the certificate is generated in a safe way and make it available to the Signer for its acceptance.

The established procedures in this section are the applicable in case of certification renewal, taking into consideration that the same involves the issuance of a new certificate.

During the process, AZIENDA ZERO:

• protects the confidentiality and integrity of the registration data that owns;

• uses reliable systems and products that are protected against every disturbance and guarantee the technical security of the processes of certification to which they support;

• generates a pair of keys, through a safe procedure of generation of the certificate ;

• uses a procedure of generation of certificates that links in a safe way the certificate with the registration information, including the certified public key;

• it ensures that the certificate is issued by systems using protection against counterfeiting and guarantees the confidentiality of the keys during the process of generation of the generation of the mentioned keys;

• Indicates the date and hour in which a certificate was issued;

• It ensures the exclusive control of the keys by the user, and AZIENDA ZERO or its R.A., so that the third parties cannot deduce or use them in any way.

4.3.2. TSU certificate issuance

The certificate request is performed manually by two system operators who operate on behalf of Azienda Zero and are involved in the technical management process of the systems.
• A system operator generates a pair of keys on the HSM partition in charge of the time stamping service. Then, it generates the CSR (Certificate Signing request) in PKCS # 10 format and saves it on a physical device (eg CD-ROM, Pen Drive). This device is ultimately passed to another system operator responsible for issuing the certificate.
• The latter operator, having received the physical support, proceeds to issue the TSU certificate using a specific CA software that allows the certificate to be signed with the TSA keys. The certificate thus generated is finally saved on a physical medium (where possible, the same as in the previous point) and returned to the first operator who completes the process with the installation of the certificate on the HSM and with the appropriate configuration of the time stamp service.

4.3.3. Certificate issuance notification

AZIENDA ZERO notifies the applicant about the certificate issuance.

4.4. Certificate delivery and acceptance

4.4.1. R.A. Responsibilities

The authorised staff of Azienda Zero Registration Authority must perform the following actions:

• Definitely confirm the identity of the natural person identified in the certificate, in accordance with the the sections 3;

• To deliver to the natural person identified in the certificate the sheet delivery and the acceptance of the certificate with the following minimum contents:

- basic information about the use of the certificate, the applicable Operating Manual, the data relating to the CA, as well as its obligations, powers and responsibilities;
- information about the certificate;
- recognition, from the signer, of receiving and accepting the data associated to the certificate use;
- signer obligation and responsibility;
- exclusive imputation method of the signer, of its private key and its certificate activation data, in accordance with the section 6;
- the date of the act of delivery and acceptance.

• To obtain the signature of the person identified in the certificate.

The R.A. are responsible for the execution of these procedures, they have to store the original documents (delivery and acceptance sheets), when Azienda Zero has the need to access them, and to send a digital copy to the supervisory body.

All of the aforementioned documents will be stored and archived, also in electronic format, by Azienda Zero with guarantees of security and integrity for a period of at least 20 years from the expiry date of the signature certificate (pursuant to art.28 co. 4-bis Legislative Decree 82 of 7 March 2005 and subsequent amendments), also in order to provide proof of certification in any proceedings of the Judicial Authority and, in any case, no later than the period established by law.

4.4.2. Certificate acceptance

The acceptance of the certificate by the natural person identified in the certificate occurs when the delivery and acceptance sheet have been signed.

4.4.3. Certificate publication

AZIENDA ZERO publishes the certificate in the Repository described in section 2, adopting the proper safety controls and whenever it had the authorisation of the natural person identified in the certificate.

4.4.4. Notification of the certificate issuance to third parties

AZIENDA ZERO does not notify any issuance to third parties.

4.5. Key pair and certificate usage

4.5.1. Use by the Subscriber and/or Signer

The signer has to:

- completely read and accept the contents of the present document before requesting the certificate;
- provide to the CA the complete and proper information during the certificate request;
- express his consent before the certificate emission and delivery;
- use the private key and the certificate only for the purposes described in this Certification Practice Statement;
- adopt security measures to prevent unauthorized use of the private key;
- ensure the confidentiality of reserved codes received from the CA;

- promptly request to the CA the suspension of the certificate in case of suspected compromise of the private key;
- in case of ascertained compromise of the private key, promptly request to the CA the revocation of the certificate;
- before using the private key, carefully check that the corresponding certificate obtained by AZIENDA ZERO has the expected profile and contains correct information, including any restrictions on use;
- until the certificate expiration date or revocation, promptly inform the CA or RA in case: the signature device has been lost, stolen or damaged; he/she has lost the exclusive control of his/her private key, for example due to the compromise of the activation data (PIN or password) of his signature private key; some information contained in the certificate is incorrect or no longer valid;
- in case of compromise of the private key (for example, due to the loss of the PIN of the signature device or its disclosure to unauthorized third parties), immediately stop using the same and make sure that it is no longer used.
  In this situation the C.A. immediately revokes the certificate.

AZIENDA ZERO forces the signer to take responsibility to ensure that:
• all the provided information, contained in the certificate, is correct;
• the certificate is used exclusively for legal and authorised uses, in accordance with the Certification Practice Statement;
• no unauthorised person has access to the certificate private key and that s/he is the sole responsible for any damage caused by the failure to protect the private key;
• not to transfer or grant the private key for use under any circumstances (since it is a strictly personal element) to third parties.

4.5.2. Relying Parties use

4.5.2.1. Relying Parties Obligations

All those who rely on the information contained in the certificates (R.P. abbreviation for Relying Parties) in compliance with the provisions of OVR-6.3.5-03 of the ETSI EN 319 411-1 / 411-2 standards, are obliged to:

• verify that the certificate has not expired;

• verify the the validity status of the certificate, i.e. its possible revocation using the current information on the revocation status. The validation must be carried out taking into account the status of the certificate at the relevant date-time for the RP, according to the particular context (e.g. current date-time, date-time of affixing the signature in the event that it can be demonstrated through a timestamp affixed to the document) .

• take into account any limitations on the use of the certificate;

• take any precautions as prescribed in the agreements or elsewhere;

The Relying Parties may also use the indicators and provisions of this manual to determine the suitability and reliability of the certificates in the framework of Regulation (EU) no. 910/2014.

4.5.2.2. Civil Responsibility of the Relying Parties

All those who rely on the information contained in the certificates are responsible for:

• having sufficient information to make decisions about the reliability of a certificate;

• accepting the truth of the information contained in the certificate;

• respecting the obligations imposed such as Relying Parties, according to the provisions of the previous paragraph.

4.6. Key and certificate renewal

4.6.1. Circumstances for certificate and key renewal

The certificates that aren't exipered, or revocated, can be renewed through a specific and simple procedure.

This consists in the generation of a new pair of keys (by the Applicant through specific tools made available by Azienda Zero) and issue of a new certificate with

- validity period equal to the validity period of the expiring certificate
- the same identification data of the Owner.

The renewal does not require a new identification of the Owner and therefore it can also be carried out independently by the latter through the use of special software made available by AZIENDA ZERO.

4.6.2. Renewal procedure

The Applicant can request a renewal of the certificate in the event that the identification data has not changed or, in any case, in the event that the life cycle of the certificate is close to expiry.
The renewal procedure consists of the following steps:

- the Subscriber sends the CA an authenticated renewal request with an advanced electronic signature, generated with the private key of the pair of keys to be renewed, so as to allow the latter to verify the identity of the Subscriber;
- the Operator or Operators authorized by AZIENDA ZERO R.A. verify that the information provided during the identification of the Subscriber and / or the Owner continues to be valid and have not undergone changes.

If, in the qualified Certificate, information relating to the Role and Organization to which the Subscriber belongs is also present, the CA will insert it in the new certificate, verifying, at the time of renewal, that the certificate has not been revoked by the Third Party concerned. .
In these cases the CA, in addition to verifying any cases of revocation of the certificate due to security breaches, is required to verify the existence and validity of the certificate to be renewed as well as the validity of the information used to identify the holder.
The renewal of the certificate will be notified by the CA to the Applicant by e-mail to the last e-mail address communicated.
The Applicant who has received the new certificate can no longer use the private key relating to the old certificate.
Once expired or revoked, the certificate can no longer be reissued but a new issue of the certificate is required in the same way as described for the first issue (see par. 4.1, 4.2 and 4.3).

4.7. Key Changeover (certificate re-key)

The the certificate rekeying is not allowed under any circumstances by AZIENDA ZERO.

4.8. Certificate modification

Certificates modification, that occurs when the Signer's information change (with the exception of the modification of the public key, which involves a renewal), will be managed as an ex novo issue, accordingly to the sections 4.

4.9. Revocation of certificates

The revocation of a certificate means the early and final termination of its validity. Therefore, revocation is an irreversible condition.

4.9.1. Hypothesis of revocation of a certificate

AZIENDA ZERO revocates a certificate in the following cases:

1) Circumstances affecting the information contained in the certificate:
   a) modification of any of the data contained in the certificate, after the corresponding certificate issuing;
   c) presence of incorrect data inside the certificate.

2) Circumstances affecting the security of the key or certificate:
   a) compromise of the private key, the infrastructure or the Cerificate Athority that issued the certificate, when this situation affects the reliability of the issued certificates;
   b) violation, by Azienda Zero, of the requirements of the certificate management procedures established in this Certification Practice Statement;
   c) certain or suspected compromise of the security key or issued certificate;
   d) unauthorised access or use, by third parties, of the private key corresponding to the public key contained in the certificate;

e) irregular use of the certificate by the natural person identified in the certificate or lack of diligence in the custody of the private key.

3) Circumstances affecting Subscriber and/or Signer:

a) suspension of the contract between the CA and the Subscriber and/or Signer;

b) modification or early suspension of the contract between the CA and the Subscriber and/or Signer;

c) violation by the Subscriber of the certificate of the pre-established requisites for his request;

d) violation by the Subscriber and/or Signer of the contractual obligations;

e) subscriber and/or Signer' incapacity;

f) expilcit request for revocation of the certificate by the Subscriber and/or Signer, in accordance with the provisions of section 3.

4) Other circumstances:

a) termination of the Certification Service by C.A. AZIENDA ZERO;

b) use of the non-conforming and prejudicial certificate for Azienda Zero, especially on an ongoing basis.

In this case, a use is considered demaging according to the following criteria:

o the nature and the number of complaints received;

o the identity of the subjects presenting the complaints;

o the applicable legislation;

o the reply provided by the Applicant with respect to the complaints received.

4.9.2. Who can request revocation

The revocation of a certificate can be requested by the Subscriber and the subjects indicated in Par. 4.9.1., n. 3 lett. f) through the intervention of the Registration Operator in the following ways.

4.9.3. Procedure relating to the request for revocation

The person who requests the revocation of a certificate can do so by contacting AZIENDA ZERO or the R.A., or in first person, through the online service available on the AZIENDA ZERO web page. The request for revocation must include the following information:

• date of request for revocation;

• identification data of the Subscriber;
• contact details of the person requesting the revocation;
• detailed motivation regarding the request for revocation.

Before proceeding with the revocation the request must be validated by AZIENDA ZERO, in accordance with the requirements established in paragraph 3 of the present Certification Practice Statement.

The revocation service is available on the AZIENDA ZERO website at https://azero.veneto.it/ca/.

Following the processing of the revocation request, the change of status of the certificate will be notified to the Applicant.

The revocation system is considered a critical service included in the emergency and business continuity plan of AZIENDA ZERO.

4.9.4. Duration of the request for revocation

The requests for revocation will be processed at the same time as the CA becomes aware of it.
AZIENDA ZERO performs the revocation with timeliness and attention, ensuring that the time necessary for the revocation operation and the consequent updating of the status of the certificate (carried out by publishing a new CRL revocation list) is as short as possible.

4.9.5. Duration of the request for revocation elaboration

If made by an Operator, the revocation request will be processed within the usual business hours of AZIENDA ZERO or where applicable by R.A. who proceeded to issue the certificate.
If made online, it will take effect immediately.
If Azienda Zero receives a revocation request, it is processed immediately to minimize the time after which the revocation becomes effective (which coincides with the publication of the certificate in a new CRL).
The revoked certificate is inserted into the CRL within 1 hour of revocation and in any case under no circumstances beyond 24 hours following the operation.

4.9.6. Obligation of verifying the information concerning the revocation of certificates

All those who must rely on the information contained in the certificates (so-called "Relying Parties") have the obligation, before accepting a certificate, to verify that the latter has not been revoked or expired at the date of the verification.

One method to carry out this check is to consult the most recent Certificate Revocation List (CRL) issued by AZIENDA ZERO.

The Certificate Revocation Lists are published in the CA Repository and at the following addresses (URLs):

- http://crl1.uanataca.com/public/pki/crl/azeroCA.crl;
- http://crl1.uanataca.com/public/pki/crl/azeroTSA.crl;
- http://crl2.uanataca.com/public/pki/crl/azeroCA.crl;
- http://crl2.uanataca.com/public/pki/crl/azeroTSA.crl.

The aforementioned addresses are shown in each of the certificates issued by AZIENDA ZERO, in the "CRL Distribution Point" section.
The verification can also be performed by querying the OCSP service provided by AZIENDA ZERO to the following addresses:

- http://ocsp1.uanataca.com/public/pki/ocsp/;
- http://ocsp2.uanataca.com/public/pki/ocsp/.

4.9.7. Frequency of CRL issuance

AZIENDA ZERO issues a new CRL at least every 24 hours, even in the absence of new requests for revocation

4.9.8. CRL publication

The CRLs are published immediately after their creation. The latency between the moment of the CRL creation and that of its publication under no circumstances exceeds 60 minutes.

4.9.9. Availability of revocation online verification services

AZIENDA ZERO makes available, in addition to the publication of the CRLs, an online verification service of the status of the certificates based on the OCSP protocol (RFC 6960).
The OCSP service is accessible 7x24.
In the event of a malfunction of the certificate verification systems, AZIENDA ZERO undertakes to ensure that the service remains inactive for as little time as possible. In any case, the unavailability time of the online revocation verification service cannot exceed 6 hours.

4.9.10. Other forms of publication of the revocation

There is no further method of publication of the revocation apart from those provided in section 4.9.

4.9.11. Special conditions in case of compromise / corruption of the private key

Unavailable.

4.9.12. Circumstances for suspension

The suspension of the qualified electronic signature certificate is not foreseen under any circumstances.
The suspension for TSU certificates is not foreseen under any circumstances.

4.10. Information Services on the status of the certificates

The status of qualified certificates is made available through the publication of the CRL via the HTTP protocol and in a format compliant with the specification [RFC 5280].
The status of the certificates is also made available online through a service based on the OCSP (On-line Certificate Status Protocol) in accordance with the specification [RFC6960].
The addresses for accessing the revocation services are included in the certificates.
The CRL address is entered in the CRLDistributionPoints extension.
The OCSP server address is entered in the AuthorityInformationAccess extension.
The Services are publicly accessible.

4.11. Termination of the contract

The contract between the CA and the Owner is considered terminated upon the expiration or revocation of the certificate, except in the case of any different conditions foreseen in the contracts stipulated with some customers.
The renewal of the certificate determines the continuity of the contractual performance by the CA.

4.12. Key escrow and recovery of the private key

4.12.1. Key deposit and recovery policy and services

As part of the certification service described here, the "key escrow" of the Holders' keys is not provided. It is therefore not possible to recover the owner's private key ("key recovery") under any circumstances
As for the CA and TSA keys, recovery is instead foreseen in emergency circumstances (e.g. failure of HSM equipment). The restoration is carried out following the procedures provided by the HSM used.

4.12.2. Content Policy and Services and Session Key Recovery

No provision.

5. Physical and operational security measures

5.1. Physical Security

The AZERO ZERO certification system is located at QTSP Uanataca S.A.
Uanataca is a Bit4id group company, outsourcee designated by AZIENDA ZERO for the services covered by this document.
The outsorcee has implemented a security system related to the information system of the digital certification service characterized by physical security measures aimed at protecting the infrastructure and processing systems used to support the trust services provided.

In this context, Azienda Zero ensures:

- control of physical access;
- protection against natural disasters (eg. floods);
- continuity of power supply;
- redundant Internet connectivity (double line);
- fire and anti-flooding systems;
- anti-theft protection;
- optimal ventilation and air-conditioning;
- adoption of a policy regarding the unauthorized release of material, information, support and any further application relating to components used for fiduciary and CA services.

The constant monitoring of infrastructure and services, or the timely intervention in case of need, is guaranteed by qualified system staff who works 24h-365 days a year and assures assistance in the 24 hours following the report.
AZIENDA ZERO, through the Outsourcee, uses data center services and associated communication services (such as housing, Internet connectivity, physical security) offered by the ADAM company.
These services are certified according to the rules:
- ISO / IEC 27001: 2017
- ISO 9001: 2018.
The Datacenter is located at: C / del Artesans, 7 - 08290 Cerdanyola de Vallés, Barcelona (Spain).

5.1.1. Location and implementation of structures

The infrastructures protection, that allow the provision of certification services, is assured by creating clearly defined and identifiable security perimeters.
The installations are located in areas with low risk of natural disasters (very low level of seismic risk, no volcanic risk, low risk of floods).
The quality and solidity of the installations construction materials ensure adequate levels of protection against forced intrusion attempts and allows quick access for any emergency actions.

The room where the cryptographic operations are carried out in the Data Processing Center boasts infrastructures with very high technological requisites, as well as various alternative sources of electricity and cooling in case of emergency.

Outsourcee has facilities that physically protect the environments in which the operations of trust services provision are carried out.

5.1.2. Physical access

Suppliers have implemented a physical security system on three levels:
- access to the building where the CED is located;
- access to the hall;
- access to the Rack;

for the protection of the trust services provided.

The physical access to the spaces where the certification processes take place is protected through a combination of physical and procedural measures.
This access in particular:

- is limited to authorized staff, with access authentication, registration, CCTV video recording and archiving ;
- is realized with badge readers and it is managed by an information system with tracking (and relative generation of evidences and logs) of entry and exit.

In addition, the access to the rack where the cryptographic modules and the "core" of the infrastructure are located takes place only with prior authorization from the Management of the Outsorucee or the Security Manager.

5.1.3. Electricity and air conditioning

The facilities in which is performed, in outsourcing, the certification service have the equipment to stabilize the current and an electrical supply system supported by a power generator.
The areas that house the computer equipment have temperature control systems with air conditioning.

5.1.4. Exposure to water

The machines are in an area with a low risk of flooding.
The rooms where the computer equipment are located have a humidity detection system.

5.1.5. Prevention and fire protection

The equipment and material have an automatic system for identifying and extinguishing fires.

5.1.6. Storage devices

Only the authorized personnel have access to the storage devices.
The upper level information is stored in a strongbox outside the Data Processing Center facilities.

5.1.7. Waste disposal

The elimination of paper and magnetic materials is carried out through mechanisms that guarantee the impossibility of retrieving information.
In the case of magnetic material, this is physically destroyed or reused after the secure cancellation of the contents.
In case of paper documentation, the deletion of information is done through shredding machines or baskets that are subsequently destroyed under strict control.

5.1.8. Backup copy external to the structures

Suppliers use a secure external file for the custody of documents, magnetic and electronic devices independent from the Operations Center.

5.2. Controls on procedures and operational security

AZIENDA ZERO guarantees that its systems operate in a safe way, therefore it has established and introduced procedures that rigorously regulate the performance of its services.

The staff of AZIENDA ZERO performs the administrative and management procedures in accordance with the security policy established by AZIENDA ZERO.

5.2.1. Trust roles

In compliance with the current regulations, with the ETSI EN 319 401 and ETSI EN 319 411-1 standards and with its own safety policy, AZIENDA ZERO has established the following positions or roles of trust:

- **Responsible for the security**: in charge of coordinating, monitoring and enforcing the security measures defined in the security policy of AZIENDA ZERO. This figure must take care of the aspects related to the information security: logistics, physics, network, organizational, etc.;
- **Internal auditor**: responsible for carrying out operational procedures. This figure is also responsible for verifying the archives and audit logs of the CA systems;
- **System administrator**: responsible for the installation, configuration, maintenance and proper functioning of the systems for the provision of trust services;
- **System operator**: responsible for the daily operation of the proper functioning of the systems for the provision of trust services;
- **Registration operator**: responsible for approving the requests for issuing a certificate forwarded by the Applicant and/or Signer; responsible for verifying the necessary information and applying the procedures defined by Azienda Zero for the issue of digital certificates or for the provision of trust services;
- **Revocation operator**: responsible for updating a certificate status of validity (eg. revocation).

People who fulfill the roles listed above are subject to specific control and safety procedures. Furthermore, the division of roles, according to the criteria defined in the organizational context of AZIENDA ZERO, is a measure to prevent fraudulent activities.

5.2.2. Number of people per activity

AZIENDA ZERO, with the technological partner support, guarantees at least two people to carry out activities related to the generation, recovery and back-up of the Certification Authority private key.

5.2.3. Identification and authentication for different roles

People assigned to each role are identified by the internal auditor who ensures that each one carries out the operations assigned.
Each employee only checks the activities related to his/her role, thus ensuring that no one accesses the resources that have not been assigned to him/her.
The access to the resources, depending on the activity, is performed through user name/ code, digital certificate, badge and / or key.

5.2.4. Assignements that require separation of tasks

The following tasks are performed by at least two people:

- the duties of the Internal Auditor are incompatible with those relating to the administration of systems and, in general, with the operations related to the implementation of electronic trust services;
- the tasks related to the issue and revocation of certificates are incompatible with those concerning the administration of the systems.

5.2.5. PKI management system

The PKI system consists of the following modules:

- component /management module of the Certification Authority;
- component /management module of the Registration Office;
- component /request management module;
- key management component /module (HSM);
- database component / module;
- CRL component / management module;
- component / management module of the Validation Authority.

5.3. Personal Security

5.3.1. Qualification, experience and required authorizations

The AZIENDA ZERO staff, similarly to that of of its technological partner, is highly qualified and/or has been duly trained to carry out the operations assigned.

The staff with a trusted role have no personal interests that conflict with the performance of the role assigned.

AZIENDA ZERO ensures that the registration staff is reliable for carrying out the registration tasks. The registration manager receives information to perform the task of requests validating.

In general, AZIENDA ZERO will relieve an employee from its trust position if aware of the existence of conflicts of interest and/or the commission of any unlawful act having effect on the performance of his/her duties.

AZIENDA ZERO will not assign a confidential or management task to a not reliable person. For this reason, **within the limits of the legislation in force**, a preliminary investigation will be carried out on the following aspects:

- studies, including the titles to be attached;
- previous jobs (up to five years);
- professional references.

In any case, the R.A., being responsible for the people authorized to carry out its activities, may establish further procedures for the verification of the above requirements, always in compliance with the AZERO ZERO policy.

5.3.2. Procedures for verifying the staff information

AZIENDA ZERO, before hiring a person or allowing him / her access to the workplace, makes inquiries concerning:

- references on jobs carried out in recent years;
- professional references;
- studies, including attached titles.

AZIENDA ZERO obtains, before the conduct of these investigations, the express consent of the interested party, undertaking to treat and protect the personal data of these subjects, in compliance with the current legislation on the protection of personal data, pursuant to European Regulation no. 2016/679 and to the current national legislation.

All checks are carried out in compliance with the current legislation.
The reasons that may lead to the refusal of the candidate are the follows:

- false statements made by the candidate in the curriculum vitae;
- negative and/or unreliable professional references.

5.3.3. Training requirements

AZIENDA ZERO adequately trains the staff assigned to positions of trust and management, until reaching the qualification to be filled, keeping track of the aforementioned training.
Training programs are periodically reviewed, updated and improved.
The training includes at least the following contents:

- security principles and mechanisms of the certification hierarchy;
- tasks that the person must perform;
- AZIENDA ZERO security policies and procedures;
- use and interventions on installed machinery and applications;
- management and resolution of incidents and safety compromises;
- business continuity and emergency procedures;
- management and safety procedures in relation to the processing of personal data.

5.3.4. Requirements and attendance of training

Especially when substantial changes are made to the tasks related to certification services, AZIENDA ZERO updates its staff in an accurate and satisfactory manner.

5.3.5. Tasks rotation

Not applicable.

5.3.6. Penalities for unauthorized actions

AZIENDA ZERO implements disciplinary procedures when it is necessary to establish the responsibilities come from unauthorized actions, within the limits and in compliance with applicable labor law provisions.

Proportionally to the severity of the unauthorized action, disciplinary actions include suspension, separation of duties until the termination of the contractual employment relationship.

5.3.7. Requirements for hiring qualified personnel

Employees recruited to carry out trusted tasks sign the confidentiality clauses and the operational requirements used by AZIENDA ZERO in advance. Any action that compromises the safety of the accepted procedures, may, after evaluation, give rise to the termination of the employment contract.
In the event that all the certification services, or part of them, are carried out by third parties, they have to comply with the controls and provisions provided in this or other sections of the Certification Practice Statement. The division of responsibility between the CA and these subjects is defined by a special agreement between the Parties.

5.3.8. Documentation submission to the staff

The Certification Service Provider will provide the necessary documentation to its staff, so that the latter can perform its activities in a competent and effective manner.

5.4. Safety control procedures

5.4.1. Types of registered incidents

AZIENDA ZERO produces documents and safety information, at least with regard to the following incidents, related to the security of the Certification Authority:

- system start and stop;
- attempts to create, delete, reset password or change rights;
- attempts to access and stop the session;
- attempted unauthorized access to the CA system through the network;
- unauthorized attempts to access the storage system;
- physical access to logs;
- change of system configuration;
- CA application log;
- fire and extinction of the CA application;
- CA and / or its keys modification;
- change in the creation of rules related to the certificates;
- generation of own keys;
- creation and revocation of certificates;
- log on the destruction of devices containing keys and related activation data;

- events related to the life cycle of the cryptographic module, such as release and use of the same;
- the generation of keys and key management databases;
- physical access registers;
- maintenance and changes in system configuration;
- change of personnel;
- reports on compromises and discrepancies;
- log on the destruction of material that contains information on keys, activation data or personal information;
- comprehensive reports on attempts of physical intrusion into infrastructures that support the certificates issuance and management.

The registry entries include the following elements:

- date and time;
- serial number or sequence of entry into automatic registers (log);
- identity of the person making the access;
- type of access.

5.4.2. Frequency of control journal elaboration

AZIENDA ZERO checks the logs when a system alert is produced due to an incident.
The control journal elaboration consists in the review of the latter, aimed at ascertaining the non-manipulation of the same, a brief inspection of all registered accesses and a deeper investigation aimed at the analysis of potentially dangerous events.
The actions performed for the analysis of the audit journal are documented.
AZIENDA ZERO has a system that allows to guarantee:

- that there is sufficient space for storing logs;
- that the logs are not rewritten;
- that the log records at least the type of event, date and time, user and result of the operation.

5.4.3. Control journal conservation period

AZIENDA ZERO stores information from the control journal for a period of 20 years.

5.4.4. Verification records protection

Systems Logs:

- are protected through digital signature against manipulation;

- are housed in fireproof devices.

Access to the logs is reserved exclusively to authorized personnel.

There is an internal procedure in which the devices management processes, that contain control log data, are detailed.

5.4.5. Backup procedures

AZIENDA ZERO has a reliable backup procedure so that, in case of loss or destruction of important records, the respective backup copies of the logs are available for a short period of time.

AZIENDA ZERO implemented a safe backup system procedure of the control logs by making a weekly copy of all logs in an external environment. Furthermore, a copy is kept in an external custody center.

5.4.6. Control journal storage system

The information relating to the control journal is automatically memorized through the use of utilities developed ad hoc by AZIENDA ZERO.

Only the designated staff can ask the system administrators for the control journal, which is automatically signed and encrypted automatically by the aforementioned utilities.

It is possible to decrypt the logs only through specific devices.

These devices are securely stored in a strongbox and only the internal auditor knows the related PIN (moreover it is put in a sealed envelope, in the same strongbox).

5.4.7. Notification in case of suspicious event

No stipulation.

5.4.8. Vulnerability analysis

The analysis of potential vulnerabilities of the AZIENDA ZERO infrastructure is subject to the control procedures implemented by the same.

The vulnerability analysis must be performed, examined and reviewed to make an assessment of the developments necessary to resolve them. These analysis are periodically carried out in accordance with the internal procedure provided for this purpose. System verification data is stored to be used for incident investigations and for identify vulnerabilities.

5.5. Information storage

AZIENDA ZERO guarantees that any information related to certificates is stored for an appropriate period of time, in accordance with the current laws.

5.5.1. Types of records stored

The following documents involved in the certificate life cycle are stored by AZIENDA ZERO (or by R.A.):

- all audit data system;
- all data related to certificates, including contracts with the signers and data related to their certification and location;
- certificates issuance and revocation requests;
- type of document presented in the certificate request;
- identity of the Registration Authority that accepts the certificate request;
- all certificates issued or published;
- issued CRLs;
- certificates status logs;
- generated keys history;
- communications among the PKI elements;
- certification policies and practices;
- information on certification requests;
- documentation provided to justify the certification requests;
- information on the certificate life cycle.

AZIENDA ZERO and/or R.A., as the case may be, are responsible for the correct storage of all the above mentioned material.

5.5.2. Registers storage period

AZIENDA ZERO stores the above mentioned registers for at least 20 years, or in accordance with the current laws.

In particular, the revoked certificates registers will be accessible for consultation for at least 20 years or in accordance with the laws in force at the time of revocation.

5.5.3. Archives protection

AZIENDA ZERO protects archives so that only duly authorised persons can access to them. Archives are protected against visualisation, modification, cancellation or any other manipulation, through its storage in a reliable system.
AZIENDA ZERO ensures proper protection of archives by assigning qualified personnel for their treatment and storage in secure external facilities.

5.5.4. Back-up procedures

AZIENDA ZERO has an external storage centre to ensure the availability of electronic files backups. Paper documents are stored in safe places, restricted to authorised personnel.
AZIENDA ZERO makes incremental daily backups of all electronic documents and weekly full backups to ensure data recovery.
In addition, AZIENDA ZERO (or Registration Offices) keeps a copy of the paper documents in a safe place separated from the Certification Authority facilities.

5.5.5. Timestamping requirements

Records are dated with a reliable source via NTP.
There is no need to digitally sign this information.

5.5.6. Storage system localization

AZIENDA ZERO has a centralised system to gather information on the activity of the team involved in the certificates management service.

5.5.7. Procedures to obtain and verify archiving information

AZIENDA ZERO has a procedure that describes the process to verify that the stored information is correct and accessible. AZIENDA ZERO provides information and means for verification to the auditor.

5.6. Keys renewal

At least 5 years before the expiration of the validity of the CA's private key and at least ten years before the expiry of the last certificate issued, AZIENDA ZERO will generate a new pair of CA keys.

The selfsigned certificate corresponding to the aforementioned key pair is sent to the National Supervisory Body of Trust Service Providers (AgID).

After the insertion of the new CA certificate in the trusted list (TSL) published by the previously mentioned Supervisory Body, AZIENDA ZERO begins to sign the new certificates and the corresponding CRLs with the new CA key.

The old CA and its private key will only be used for CRL signing.

The relative period of validity of the certificate is therefore determined on the basis of:

- the technological state;
- the state of the art of cryptographic knowledge;
- the intended use for the same certificate;

Any replacement of the CA private key will result in a modification to this manual and related communication to the competent Supervisory Authority (AgID).

5.7. Keys compromise and disaster recovery

5.7.1. Disasters and compromises management procedures

AZIENDA ZERO, with the Outsourcers support, has developed security and business continuity policies, allowing the systems management and backup in case of operations compromise or disaster. This ensures critical services for revocation and publication of the certificates status.

5.7.2. Resources, applications or data corruption

In case resources, applications or data are corrupted, specific management procedures, according to AZIENDA ZERO security and incidents management policies, will be activated. They include scaling, investigation and response to the incident. If necessary, AZIENDA ZERO keys compromise or disaster recovery procedures will be activated.

5.7.3. CA private key compromise

In case the compromise is suspected or found to be present by AZIENDA ZERO, keys compromise procedures will be activated in accordance with the security policies and the incidents and business continuity management, allowing the recovery of critical systems, and, if necessary, the recovery in an alternative data centre.

5.7.4. Business continuity after an incident

AZIENDA ZERO adopts all the procedures necessary to guarantee the continuity of the service also following highly critical situations through the use of reserve systems.

The plan applies to the DR center designated by Azienda Zero, which provides sufficient system redundancy to meet the availability requirements of the systems envisaged and the restoration of the processing services on the Disaster Recovery site.

AZIENDA ZERO will restore the critical services (revocation and publication of the information on the status of the certificates) in accordance with the existing criticality and operational continuity plan (compliant with the ISO / IEC 27001 standard), thus ensuring the expected operation of the services within the terms set by the aforementioned continuity plan.
AZIENDA ZERO has a DR center, where availability for the implementation of the certification systems described in the business continuity plan is needed, located at the datacenter of the outsource company, Bit4id s.r.l in via Diocleziano n. 107 - Naples.

5.8. Service cessation

AZIENDA ZERO assures Applicants and / or Holders and Relying Parties that any interruptions, following the temporary cessation of the certification services performed by the CA, are minimal. In this way, AZIENDA ZERO guarantees continuous maintenance of the registers for the time established in section 5 of this Operating Manual.
However, AZIENDA ZERO will carry out all the necessary actions to transfer the maintenance obligations of the registers indicated above to third parties or to a notary, for an appropriate period, based on the requirements of this Operating Manual and the regulatory provisions relating to the provision of trust services.
Before ceasing the provision of Certification Services, AZIENDA ZERO develops a plan to cease operations, with the following provisions:

- provide the funds necessary to continue the cessation activities;
- notify all Signers/Applicants, third parties and other CA with which they have agreements or any other type of relationship, of the cessation with at least 60 days before the scheduled service cessation date;

- revoke any authorisation to outsourced Authorities to act on behalf of the CA in the process of certificates issuance;
- transfer obligations regarding the maintenance of the registries and logs information for the time period specified to Signers and users;
- destroy or disable the CA private keys;
- keep the certificates and the verification and revocation system active until the issued certificates expire;
- perform the activities necessary to transfer the maintenance obligations of the registries information and event log files for the respective time periods specified to the contractor and relying third parties using the certificates;
- notify the competent Supervisory authorities, at least 60 days in advance, of the activity cessation and the certificates destination, specifying if the management is transferred and to whom or if the validity will expire;
- notify the competent Supervisory authorities of the initiation of any insolvency proceeding against AZIENDA ZERO, as well as any other relevant circumstance that can prevent the activity continuation.

6. Technical security measures

AZIENDA ZERO uses reliable systems and techniques to guarantee the technical safety of the implemented processes. All the technical safety measures employed by AZIENDA ZERO comply with the following reference standards:

- ETSI EN 319 411-1
- ETSI EN 319 411-2
- ETSI EN 319 421

6.1. Generation and installation of the key pair

6.1.1. Generation of the key pair

6.1.1.1. CA keys

The CA key pair is generated following a "key ceremony" procedure that takes place in a protected environment, within a high security perimeter specifically designed for that purpose.

The activities carried out during the "ceremony" of generation of the certification keys are recorded, dated and signed by all the people involved. In addition, the execution of these activities takes place in the presence of the internal auditor and is documented in a special report prepared by the safety manager.
The minutes are kept for control and monitoring purposes, for an appropriate period defined by AZIENDA ZERO.
FIM 140-2 level 3 and Common Criteria EAL4 + compliant HSM devices were used to generate the keys.

Azienda Zero CA eIDAS 1 Qualified	4.096 bits	25 years
- Final entity certificates	2.048 bits	Up to 3 years
Azienda Zero TSA eIDAS 1 Qualified	4.096 bits	25 years
- Time Stamping Unit Certificates	2.048 bits	Up to 8 years

6.1.1.2. Signers keys

The Holders' keys are generated through secure hardware devices (QSCD - Qualified Signature Creation Device), in accordance with what is indicated in the "security target" of the device itself and through the software libraries provided by the device manufacturer.

The algorithms and cryptographic suites used comply with the ETSI TS 119 312 specifications.

In particular, the keys are generated using the RSA public key algorithm, with a minimum length of 2048 bits

signer keys can be generated through hardware and/or software devices, authorised by AZIENDA ZERO.

The keys that are not generated by a QSCD will be created by the Signer through applications and procedures defined by AZIENDA ZERO.

AZIENDA ZERO never creates keys to be sent to the signer outside of a QSCD.

The keys are created using the RSA public key algorithm, with a minimum length of 2048 bits.

6.1.1.3. TSU Keys

TSU keys are generated in a physically protected environment, in accordance with the internal procedures of AZIENDA ZERO relating to time stamping systems.

The execution of these activities takes place in the presence of the internal auditor and is documented in a special report.

The device used for the generation and storage of TSU keys is certified in compliance with the FIPS PUB 140-2 Level 3 security standard

6.1.2. Delivery of the private key to the Signer

In the case of certificates relating to keys residing on a QSCD (qualified device for creating the signature), the private key is generated and stored in a protected manner within the aforementioned qualified device.

In the certificates present in a remote QSCD, the Owner's private key is generated in a remote HSM, within a private section intended for the Owner.

Access to the private key takes place through application interfaces exposed by the device and exclusively through a secure authentication procedure.

The credentials for accessing the private key are entered by the Data Controller and are not stored nor can they be deduced or intercepted by the remote generation and custody system.

The private key is not sent to the Owner, therefore it never leaves the security environment that guarantees the exclusive control of the private key by the Signer.

6.1.3. Delivery of the public key to the CA

The public keys of AZIENDA ZERO are communicated to third parties who use the certificates, ensuring the integrity of the key and authenticating its origin, through publication on the official website https://azero.veneto.it and through publication on the Trust -Service Status List (TSL) carried out by the National Supervisory Body (AgID).

6.1.4. Keys lenght

• The length of the CA keys is 4096 bits;

• The length of the keys of the end user certificates is 2048 bits. The key length of TSU Certificates is 2048 bits.

6.1.5. Generating public key parameters

The public key of the root, subordinate CAs and certificates of the Holders and TSUs is coded in accordance with the RFC 5280 standard.

6.1.6. Quality check of the public key parameters

- Module Length = 4096 bits;
- Keys Generation Algorithm: rsagen1;
- Cryptographic summary functions: SHA256.

6.1.7. Key generation in IT applications or capital goods

Keys are generated through tools and procedures, as outlined in the section 6.

6.1.8. Keys purposes

Keys for the certificates issued by CA are exclusively used to sign certificates and CRL.
Keys for the end users certificates are exclusively used for non-repudiation (content commitment).

6.2. Private key protection and cryptographic module security

6.2.1. Cryptographic modules standards

In relation to the modules that manage the AZIENDA ZERO keys, the contractors of the electronic signature certificates and the TSU keys, the level required by the standards indicated in the previous paragraph 6.1 is guaranteed. (and sub paragraphs).
In particular, the CA private keys are generated and used within HSM devices with FIPS PUB 140-2 certification at Level 3 and certification and Common Criteria (ISO 15408) level EAL4 + higher.
The owner's private key resides within a Common Criteria certified hardware cryptographic device level EAL4 + or higher, appropriate for the intended use of the keys, in accordance with current legislation.

6.2.2. Private key multi-person (n of m) control

A multi-person control is required to activate the CA and TSA private key.
In the case of the CA and TSAdi ZERO COMPANY private key, the simultaneous presence of at least 3 of the 6 people who participated in the corresponding key ceremony is required. Cryptographic devices are physically protected as set out in this document.

6.2.3. Private key repository

Not allowed.

6.2.4. Private key backup

AZIENDA ZERO makes a backup copy of the private keys of the CA and TSA which makes it possible to recover them in case of criticality, loss or damage.
Both generation and recovery of the copy require the participation of at least three people.
These backup files in a safe place, different from where the operational copy is located.

6.2.5. Private key storage

CA private keys are stored for a period of 10 years after the last certificate is issued.
The aforementioned private keys and the related information will be securely stored on the servers and systems of Uanataca S.A., QTSP and technological partner of Azienda Zero to which the same has conferred a specific task for the storage and conservation of these.
Azienda Zero guarantees possession in Uanataca S.A. of all the requisites and the necessary authorizations for the management of the archived private keys to take place in compliance with the highest security standards, ensuring that the information is kept in safe fireproof archives and physically isolated from the rest of the infrastructures and within the center of custody.

6.2.6. Private key transfer into a cryptographic module

Private keys are generated directly in the cryptographic production modules of AZIENDA ZERO.
The backup and restore operations of the CA and TSA keys are carried out as specified in section 6.2 of this document.

6.2.7. Private key storage into a cryptographic module

The private keys of the CA are generated in the HSM cryptographic modules, which guarantee the security, confidentiality and impossibility of exporting the keys in the manner described in section 6 of this document.

6.2.8. Private key activation mode

AZIENDA ZERO private key is activated by carrying out the corresponding secure start procedure of the cryptographic module (as indicated by the manufacturer and running to the device's safety target), by the people indicated in section 6.

6.2.9. Private key destruction mode

Before the CA and TSA keys are destroyed, their certificates are revoked. Devices that contain part of the AZIENDA ZERO private keys will be destroyed or restarted at a low level. The deletion will follow the steps described in the cryptographic device administrator manual.

Finally, the backup copies will be destroyed safely. These operations are conducted exclusively in circumstances that make them necessary, such as in the event of termination of the service.

6.2.10. Private key deactivation mode

No stipulate.

6.2.11. Cryptographic modules classification

See paragraph 6.1.

6.3. Other aspects of the key pair management

6.3.1. Public key storage

In accordance with paragraph 5 of this document.

6.3.2. Public and private keys usage periods

Usage periods of the keys are determined by the duration of the certificate, after which they cannot be used.

6.4. Activation data

6.4.1. Generation of activation data

The activation data of the devices that protect the CA and TSA private keys of AZIENDA ZERO are generated in accordance with the provisions of section 6 and with the key ceremony. The creation and distribution of these devices is registered.
Likewise, AZIENDA ZERO generates activation data securely.

6.4.2. Activation data protection

The activation data of the devices that protect the private keys of CA and TSA are protected with PIN, the knowledge of which is restricted exclusively to the holders of the cards of the Administrative Card Set of the cryptographic modules used, as indicated in the key ceremony document . The activation data of the private keys relating to qualified signature certificates are protected during the issue so that the owner is the only one who

knows them. The owners are responsible for the safe management and protection of private activation data, preventing their disclosure to unauthorized third parties.

6.5. Cyber security checks

AZIENDA ZERO uses reliable systems to offer certification services, made available to the technological partner and QTSP UANATACA S.A.

AZIENDA ZERO and UANATACA carry out IT checks and verifications in order to establish a management of IT resources in compliance with the security level required for the management of digital certification systems and specifically to what is required by the technical standards ETSI EN 319 411-1 and ETSI EN 319 411-2.

As regards information security, AZIENDA ZERO makes use of the controls of the certification scheme on ISO 27001 compliant information management systems operated on behalf of the Outsourcee.

The equipment used is initially configured according to the appropriate safety profiles, as regards the aspects of:

- Operating system security configuration.
- Applications security configuration.
- Correct dimensioning of the system.
- Users and permissions configuration.
- Log registers configuration.
- Backup and recovery plan.
- Antivirus configuration.
- Network traffic requirements.

6.5.1. Specific technical requirements for cyber security

Each server used by AZIENDA ZERO includes the following functionalities:

- Access control to the subordinate CA services and privilege management.
- Imposition of the separation of activities for the privilege management.
- Identification and authentication of roles associated to identities.
- Storage of the contractor and subordinate CA history and audit data.
- Check of events related to security.
- Self-diagnosis of security related to the subordinate CA services.

- Mechanisms of keys and subordinate CA system recovery.

The above mentioned functionalities are performed through a combination of operating system, PKI software, physical protection and procedures.

6.5.2. Computer security assessment

The CA and registry applications used by AZIENDA ZERO are reliable.

6.6. Life cycle technical checks

6.6.1. Systems development checks

The applications and systems are developed, implemented and managed according to the development standards and internal change management procedures. eApplications have methods to verify the integrity and authenticity, as well as to correct the version to be used. The controls on the development life cycle are carried out in compliance with the safety requirements contained in the ETSI EN 319 411-1 and ETSI EN 319 411-2, and are further defined in the ISO 9001 quality procedures and in the ISO 27001 safety policies of the outsourcee indicated in paragraphs 1.3 and 1.3.4 of this document.

6.6.2. Security management checks

AZIENDA ZERO develops the activities necessary for the training and awareness of employees regarding safety. The materials used for training and the documents describing the processes are updated after being approved by a group that deals with safety management. In carrying out this function, an annual training plan is prepared. AZIENDA ZERO requires, through a specific contract, equivalent security measures to any external supplier involved in the provision of qualified trust services. Detailed descriptions of the network security checks performed are available as internal documents.

6.7. Network security controls

Access to devices that are part of the PKI infrastructure is protected by firewalls that implement a division of the architecture into well-defined network perimeters.
Communication between the different elements of the architecture takes place using network protocols that implement encryption (using the TSL / SSL protocols) and through the use of double factor authentication by explicitly authorized personnel. Vulnerability Assessments are also conducted periodically (by qualified personnel who are able to guarantee a sufficient level of independence with respect to the operation of the certification services) with the aim of identifying any vulnerabilities.

6.8. Engineering checks of cryptographic modules

The cryptographic modules are subjected to the engineering controls foreseen by the standards indicated in this paragraph.
The algorithms used for the generation of the keys are commonly accepted for the use of the key for which they are intended.
All the cryptographic operations of AZIENDA ZERO are carried out in modules with FIPS 140-2 level 3 certifications.modules are subject to engineering checks, in accordance with the standards outlined in this paragraph.
The algorithms used to generate keys are commonly accepted for the purposes for which they were intended.
AZIENDA ZERO cryptographic operations are performed in modules with FIPS 140-2 level 3 certification.

6.9. Time sources

AZIENDA ZERO has a procedure of time synchronisation coordinated via NTP, that has access to two independent services:

1) the first synchronisation takes place using a service based on GPS antennas and receivers that allows a STRATUM 1 level of trust (with two high availability systems);
2) the second one has a complementary synchronisation, via NTP, with the Spanish Real Instituto y Observatorio de la Armada (ROA). This ensures a difference of no more than one second with respect to the UTC time scale.

6.10. Changing of Status of a Qualified Signature Creation Device (QSCD)

Azienda Zero guarantees the application of the rules to evaluate the security of information technology products applicable to device certification for the creation of a qualified electronic signature pursuant to art. 30, par. 3, lett. a) of Regulation (EU) no. 910/2014.

The standards referred to are indicated in the annex to the Implementing Decision (EU) no. 650/2016 of the Commission of 25 April 2016.

In particular, in case of changes in the certification status of qualified signature creation devices (QSCD), AZIENDA ZERO will proceed as described below:

1. Azienda Zero has a list of various certified QSCDs, as well as a close relationship with the suppliers of these devices, in order to guarantee alternatives to the possible loss of certification of the QSCD devices;
2. in case of termination of the period of validity or loss of the certification, AZIENDA ZERO will not use these QSCDs for the issue of new digital certificates, neither in new issues, nor in any possible revocations.
3. It will immediately proceed to use QSCD with a valid certification
4. In the event that a QSCD device proves it never has been, for falsification or any other type of fraud, Azienda Zero will immediately proceed to communicate it to its customers and to the regulatory body, to revoke the digital certificates issued in these devices and to replace them by issuing them in valid QSCDs;
5. In any case in which there is evidence or there is clear evidence of a compromise of the QSCD devices, Company Zero will immediately revoke all the certificates whose key pairs have been generated using the aforementioned device, giving express notice to the owners and to any interested third parties. It will also replace the affected device with a valid QSCD.

7. Certificates, CRLs and OCSP profiles

7.1. Certificates profiles

The certificates issued according to this Manual comply with the public specification RFC 3739, based on the ITU-T X.509 v3 standard, as well as the European standard ETSI EN 319 412. The documentation relating to the profile of the certificates issued in compliance with the European standard ETSI EN 319 412 can be requested from AZIENDA ZERO.

7.1.1. Version number and certificate extensions

The certificate version is v3, based on the ITU-T X.509 standard.
The extensions characterizing the certificates issued according to this Manual are indicated, in detail, within the documentation relating to each certificate profile, available on the AZIENDA ZERO website (https://azero.veneto.it/ca/).

7.1.2. Algorithms identifiers

The certificates issued according to this Certification Practice Statement are signed with the sha256WithRSAEncryption algorithm, identified by the 1.2.840.113549.1.1.11 OID.
The public key algorithm is rsaEncryption, identified by the 1.2.840.113549.1.1.1 OID.

7.1.3. Names formats

The Subject field of the certificate contains a Distinguished Name (DN) compliant with the ITU-T X.500 standard and the ETSI EN 319 412 regulation.
The DN consists of attributes defined in the RFC 5280 public specification.

7.1.4. OID (Object Identifier)

As outlined in paragraph 1.2.1, each certificate profile, issued according to this Certification Practice Statement, is identified by a specific OID (Object Identifier).

7.2. CRLs profile

CRLs issued by AZIENDA ZERO are compliant with the RFC 5280 public specification.

7.2.1. Version number

In the Version field of the CRL the value 2 is indicated, as required by the specification outlined in the previous paragraph.

7.3. OCSP profile

The OCSP service issued by AZIENDA ZERO is compliant with the RFC 6960 public specification.

8. Compliance audit

As a Trusted Services Provider, AZIENDA ZERO is subject to periodic compliance audits.

8.1. Audit frequency

On an annual basis, an accredited Conformity Assessment Body (CAB) verifies the compliance of the CA services of AZIENDA ZERO with this Manual, with Regulation (EU) no. 910/2014 and applicable ETSI standards.
Again on an annual basis, with regard to digital certification services, AZIENDA ZERO has and carries out an internal auditing activity.
Furthermore, internal compliance checks can take place at any time, if any breach of security measures is suspected.

8.2. Auditors identities and qualifications

Conformity audits, in compliance with the ETSI EN 319 403 standard, are carried out exclusively by highly qualified skilled personnel, specialised in conducting audits relating to trusted services and employed by a Conformity Assessment Body (CAB), accredited in accordance with No 765/2008 Regulation (EC).

8.3. Relationship between CA and auditors

The relationship between the Conformity Assessment Body (CAB) and AZIENDA ZERO does not compromise the authenticity of the conformity checks, neither give rise to a conflict of interest that could distort the auditing activities carried out by the former towards AZIENDA ZERO.

8.4. Elements subject to audits

Audits activities involve the following aspects, in particular:

a) the compliance of the digital certification services rendered by AZIENDA ZERO with this Manual as well as with the additional documentation applicable to the CA service (e.g. internal operating procedures);

b) the implementation of the physical, technical and operational security measures, as well as those relating to the personnel security;
c) the compliance of this Certification Practice Statement and other applicable documents to CA services with applicable laws and regulations;
d) the setting up of an information and management system that guarantees the quality of the service provided;
e) the correct performance of the activities concerning digital certification services by the CA (e.g.: identification and authentication of subjects requesting certificates; management of related documentation; key management).

In summary, compliance audits activities involve the following aspects:
a) CA and RA operating procedures;
b) CA information systems;
c) measures to protect the data processing centre;
d) documents related to the CA services.

Subject to verification, in accordance with ETSI EN 19 401 (REQ-7.13-03), is also the accessibility of trust services by people with disabilities.
Considering the context of the Organization and the fact that the trust services issued by Company Zero are mainly intended for healthcare and administrative staff, the requirement of accessibility of the services is not considered strictly necessary for the provision of the same to the interested parties.

8.5. Follow-up actions to non-conformities

Once the report has been received, the Company Management, with the collaboration of the assessment body, examines any non-conformities found during the audits.
Depending on the nature and severity of the non-conformity, the Company Management defines the consequent action plan and the necessary corrective measures, also taking into account the internal procedures relating to non-conformities management.
In case the defined measures prove to be inadequate to correct the deficiencies found, or in case such deficiencies represent a threat to the security and integrity of digital certification services, the company Management may:

- temporarily, and for a transitional period, cease the operations in progress;
- revoke the CA key and regenerate the infrastructure;
- terminate the CA service;
- take any other necessary measure.

8.6. Communication of results

The Evaluation Body (OdV) communicates the result of the auditing activity to the Company Management of AZIENDA ZERO.

Furthermore, the report produced by the SB is sent to the national Supervisory Body.

9. Economic and legal conditions

9.1. Fees

9.1.1 Certificate issuance or renewal fees

AZIENDA ZERO has not provided rates for the issue or renewal of certificates: the reason for this is that the certification service will be provided by the latter initially only in favor of employees of the Healthcare Companies of the Veneto Region.
Currently, there is no provision for the issue or renewal of certificates in favor of third parties with respect to those indicated above.
AZIENDA ZERO, however, reserves the right to subsequently extend the service to natural/legal persons other than employees of the Local Health Authorities: in this case, it will proceed to establish completely the economic conditions of the tariffs for the certification services provided, informing appropriately applicants, by publishing them on their institutional website, ensuring their competitiveness.

9.1.2. Certificate access fees

There is no economic fee for access to published certificates. This access is free.

9.1.3. Certificate status information access

AZIENDA ZERO hasn't established any fee for access to information services (CRL, OCSP) on the status of certificates. This access is free.

9.1.4. Fees for other services

Not stipulated.

9.1.5. Refunf policy

Not stipulated.

9.2. Financial capacity

In accordance with European technical regulations, in relation to the management of the CA services and the cessation plan, AZIENDA ZERO has sufficient financial resources necessary to ensure the fulfillment of its obligations and to address any risks arising from the provision of the certification service.

9.2.1. Insurance coverage

By virtue of the strategic partnership relationship with the Outsourcee referred to in point 1.3.4 of this Manual, AZIENDA ZERO can count on the presence of a specific insurance policy stipulated in the name of the Outsourcee, with companies of verified importance in the insurance field.
The aforementioned insurance policy is stipulated for the specific exercise of the activities of *"digital and/or electronic certification services, as a certification services provider that issues qualified certificates, as well as its activity as a registration authority [...]"* and is to cover all the risks deriving from the provision of certification services, providing for a single ceiling per claim and per insurance period of €. 3,000,000.00 (three million, 00 //).

9.2.2. Other assets

Not stipulated.

9.2.3. Insurance cover for end users

Refer to par. 9.2.1

9.3. Protection of the information processed

9.3.1. Confidential information

AZIENDA ZERO undertakes to treat and handle the following information as confidential:

- Certificates requests, approved or rejected, and all other personal information obtained for issuance and maintenance of certificates, with the exception of the information that must be included in the certificates of for other reasons, according to the following paragraph, they are considered non-confidential;
- Private key of the Signers if they are generated and/or stored by the CA;

- Log of processing systems of the CA;
- Contracts with the CA;
- Audit documents, internal and external created and or/managed by the CA and its auditors;
- Business continuity and emercency plans;
- Security plans;
- All other information identified as “Confidential”.

All confidential information is treated by AZIENDA ZERO in compliance with the applicable rules, in particular of Legislative Decree n. 196/03 and ss.mm. and of Regulations (EU) 2016/679.
The CA ensures that confidential information is adequately protected physically and/or logically from unauthorized access as well as the risk of loss as a result of disasters (see the appropriate section in this regard).

9.3.2. Non confidential information

The following information is considered non-confidential:

- Certificates issued or in the process of issuance;
- Validity period of the certificate, as well as the date of issue of the certificate and the expiry date;
- Serial number of the certificate.
- Different status of the certificate (for example: awaiting generation and / or delivery, valid, revoked, suspended or expired), the start date of each of them and the reason for the change in status;
- Certificate Revocation List (CRL), and the remaining revocation status information;
- Information contained in the certificate;
- Information about Signers obtainable from the consultation of public sources ;
- Information that the Signer himself has asked the CA to make public;
- Any other information not indicated in the previous paragraph;

9.3.3. Hypothesis of information disclosure

AZIENDA ZERO discloses the information considered confidential, in accordance with the par. 9.3.1., only in cases in which a legal/ regulatory disclosure obligation exists.

The personal data of the Signer may be communicated to the police, judicial authorities, information and security bodies or other public entities, pursuant to Legislative Decree no. 196/2003 and subsequent amendments, in the event that this is required for the purposes of defense or security or the State or prevention, detection or repression of effenses.
The circumstances that legitimize the disclosure, by AZIENDA ZERO, of the confidential information and, in particular, of the personal data of the Applicants or Signers, will be duly indicated in the information on the processing od personal data prepared and issued by the CA.

9.4. Processing and protection of personal data

With regard to the processing and protection of personal data, AZIENDA ZERO complies with current legislation on the subject, both national and Community, with particular reference to Legislative Decree no. 196/03, and s.m.i. and Regulation (EU) 2016/976.

In compliance with the regulations concerning the protection of personal data, AZIENDA ZERO has illustrated, in this Certificate Practice Statement, which organisation and security procedures it has adopted in order to guarantee personal data processed by the risk of loss, destruction, forgery and unlawful processing and/or unauthorized.

Below, we make more detailed information regarding the processing of personal data by AZIENDA ZERO:

- Owner of the data processing

The owner of your personal data processing is AZIENDA ZERO, Passaggio Luigi Gaudenzio, 1, 35131 Padova PEC: protocollo.azero@pecveneto.it.
AZIENDA ZERO is the owner of personal data collected during identification and registration of users who request certificates and is therefore obliged to treat such data

with the utmost confidentiality and in compliance with the provisions of Legislative Decree no. 196/03, and s.m.i. as well as by Regulation (EU) 2016/679.

- Purpose of the data processing

The processing of personal data by AZIENDA ZERO is carried out for the following purpose:

a) supply of qualified trust services: the data are collected through the relative contract and processed in order to perform the fiduciary services requested and accepted by the contractor, according to the procedures indicated herein;
b) send questions and requests: data are collected through the contact form available on the AZIENDA ZERO website and used exclusively to manage the applications and requests received.

The personal data provided will not be processed for purposes other that those described above nor in an incompatible manner with the same.

- Legitimate basis of the data processing

The legal basis legitimating the processing of personal data of users is as follows:

a) The processing of personal data for the provision of qualififed trust services derives from the execution of the contract for the requested services, of which the user is a party;
b) The processing for handling requests is based on the consent of the interested party, expressly and unequivocally provided by the latter, having read the information on the processing of personal data. This content may be withdrawn at any time by sending an e-mail to supporto.ca@azero.veneto.it.

- Type of data

By processed data, in the context of this information, are meant the so-called "Personal Data", that is, information or fragments of information that allow the identification of the Applicant(s).

Usually these include information such as name, address of residence or domicile, e-mail address and telephone number, or other information such as, for example, the Company where the Applicant operates or serves, the role covered and the sector of activity.

- Storage and deletion of personal data

AZIENDA ZERO will keep the data of the interested parties in a form that allows them to be identified for a period not exceeding the achievement of the purposes for which the data were collected. Data relating to Certificates and/or Digital Identity will be retained for 20 years from the determination of the contract or from the expiration or revocation of the Digital Certificate or Identity, in accordance with the provisions of Article 28, co. 4bis of Legislative Decree 82/2005 and subsequent amendments Code of the Digital Administration) and of the at. 7, co.8 of the DPCM 24 October 2014 and s.m.i. The data stricly necessary for the fiscal and accounting obligations, having failed the purpose for which they were collected, will be kept for a period of 10 (ten) years as required by the relevant regulations. Service logs for Certificates and/or Digital Identity will be kept for a period of 6 (six) months in order to ensure the correct identification of service flows. After these periods, AZIENDA ZERO will delete the data of the interested parties.

- Area of communication

Data relating to the contract and to the activity relating to qualified trust services may be disclosed to commercial consultants for administrative and accounting purposes, as well as to legal consultants for possible managements of disputes.
In addition, data may also be disclosed to police bodies or judicial authorities for the purpose of ascertaining or prosecuting offenses committed by users of the telematic services, where necessary.
The data may also be processed by third parties as Registering Authority, Registration Operator as well as by persons with paper and/or digital management and filing function, formally appointed by AZIENDA ZERO as external responsible data processors.

- Rights of the data subjects

The interested party can exercise the rights referred to in art. 15 (Right of access of the interested party), 16 (Right of rectification), 17 (Right to cancellation), 18 (Right to limit

processing), 19 (Right to obtain notification from the owner of the data processing in cases of rectification or cancellation of personal data or their cancellation), 20 (Right to portability), 21 (Right of opposition) and 22 (right to refuse the automated process) of EU Reg. 2016/679.

To exercise their rights, interested parties can send a request to the email adress aagg.assicurativi@azero.veneto.it. In this request, you will need to attach a copy of your identity document and clearly state which right you wish to exercise.

The information on the processing of personal data is published on the AZIENDA ZERO website.
The certificate request requires the consent of the Applicant to the processing of their personal data by the CA.

9.5. Intellectual property rights

9.5.1. Property of certificates

AZIENDA ZERO has the intellectual property rights on the certificate issued.

9.5.2. Property of the Certification Practice Statement – Digital Certification Services

This Certification Practice Statement is intellectual property of AZIENDA ZERO. All rights reserved.

9.5.3. Ownership of the brands

The trademarks and the registered trademarks used by the Certificate Applicants are the exclusive property of their respective owners.
Certificate Applicants shall ensure that the use of information related to the certificate request does not interfere with or damage the rights of any third party, in any jurisdiction, with respect to trademarks service identification marks, trade names company names and any other intellectual property right.
The Signers and the Certificate Applicants undertake to indemnify and compensate AZIENDA ZERO against any loss or damage deriving from the use of the certificate and the information contained therein for illegal purposes, whitin which illegal interferences

are included on contractual advantages or potential advantages business, unfair competition, actions to harm another person's reputation, misleading advertising, and create confusion about natural or legal persons.

The Signers and the certificate Applicants undertake to indemnify and compensate AZIENDA ZERO against any loss or damage deriving from such interference or infraction.

9.6. Guarantees and responsabilities

9.6.1. Guarantees offered by AZIENDA ZERO

AZIENDA ZERO undertakes to:

- Provide the certification service conforming to this operating manual;
- Provide an efficient service for certificates revocation;
- Provide an efficient and reliable information service on the status of the certificates;
- Provide clear and complete information on the requirements and conditions of the service;
- Make a copy of this Certification Practice Statement available to anyome who requests it;
- Processing personal data in accordance with current regulations.

Moreover:

a) Provides with certainty to identify the Applicant of the Certification. With the issue of the certificate, AZIENDA ZERO certifies and guarantees that the identification data contained in the certificate were, on the case of issue of the certificate, accurate and true;
b) Informes the Applicants, before signing the agreement between the latter and the CA, in a complete and transparent manner, the conditions that govern the certification procedure;
c) Uses reliable security systems, aimed not only to ensure that only authorized persons can make insertions and changes but also that authenticity of the information is verifiable;
d) Guarantees correct operation and continuity of the system;
e) Provides the information required by the 2016/679 European Reg;

f) Guarantees that the collected data are not used or processed for different purposes without the express consent of the person to whom they refer.

9.6.2. Exclusion of warranties

AZIENDA ZERO has no further obligations and does not guarantee anything more than what is expressly provided for by the current legislation in this area or indicated in this Certification Practice Statement and in the General Supply Conditions relating to digital certification services.

9.6.3. Limitations of responsibilities

The obligations and responsibilities of AZIENDA ZERO are limited, exclusively, to those established by this Certification Practice Statement and the supply contract related to certification services. Without prejudice to the assumptions provided for by law, in no other case, for any reason and/or reason, AZIENDA ZERO can be held responsible towards the Applicant and/or Signer, for damages, directly or indirectly, connected to the latter, for damages, direct or indirect, data loss, violetion of third party rights, delays, malfunctions, interruptions, total or partial, which should occur in connection with the provision of the Service, where connected, directly or indirectly, or arising from:

- force majeure, accidents, catastrophic events (by way of example but not exhaustive: fires, explosions, strikes, riots, etc.);
- tampering or interventions on the Service or on the equipment carried out by the Signer and/or the Applicant and / or by third parties not authorized by AZIENDA ZERO.

9.6.4. Compensation for AZIENDA ZERO

With regard to the General Contract Conditions relating to certification services, the Data Controller is obliged to compensate the damages and losses, possibly less by AZIENDA ZERO, in the following cases:

a) false declaration in the request of the
certificate (eg. False data of the Applicant);

b) omissions relating to essential acts or facts, both in the case of negligence and in the event of intentional omission;

c) fallacious custody of the activation data (eg PIN) of your private key;

d) use of names in violation of the intellectual property rights of other subjects.

9.6.5. Compensation to contractors

Without prejudice to the provisions of the General Conditions of Contract relating to certification services, AZIENDA ZERO has, through the Outsource, a specific insurance to cover the risks of the activity associated with the provision of certification services (see par. 9.2.1).

In any case, the compensation for damages to third parties cannot exceed the total maximum annual amount of €. 3,000,000.00 (three million, 00 //) excluding a deductible of €. 500.00 (five hundred, 00 //) for each complaint.

In the event of damage deriving from the activities covered by the Contract, the Contractor must, under penalty of forfeiture:

- report it to AZIENDA ZERO within 24 hours of its occurrence, or since it became aware of it (followed by confirmation by registered letter with return receipt or Certified Electronic Mail within the following 24 hours);
- within six months of submitting the report referred to in the previous point, quantify any damage suffered and formulate the related claim for compensation.

9.6.6. Duration and termination of the contract

The provisions of this document apply from the date of acceptance by the User who takes advantage of the qualified trust services made available by Azienda Zero and which are therefore understood as fully accepted and will last until the expiry of the period of validity of the certificate issued by the CA.

The duration of the contract is however subject to the period of validity of the digital certificates issued by the CA: this circumstance determines, in case of revocation of the certificate, for any reason, the immediate termination of all effects of this contract.
A similar consequence derives from the termination of the contract which determines the revocation of the certificate by the issuing CA.

9.6.7. Transfer of the contract

The User is not allowed to transfer all or part of the obligations and rights arising from this contract.

9.6.8. Applicable law

The contract between the CA and the Applicant and/or the Signer is subject to Italian and European law and such it will be interpreted and executed. In relation to aspects not expressly provided for in the contract, certification services provided by Azienda Zero are subject to current regulations.

9.6.5. Jurisdiction

In the contract concluded with the Applicant and/or the Signer are contained clauses related to the resolution of disputes that may arise between in the Parties.

9.7. Final provisions

9.7.1. Changes to this agreement

This Manual and the provisions contained therein are likely to be modified, supplemented, replaced or eliminated by the predisposer at any time without notice to the User, except for compliance with the regulatory obligations relating to advertising.

9.7.2. Whole agreement

This Manual is capable of being supplemented or not by General Conditions or details signed specifically by the User, subject to agreement with the CA, and constitutes the discipline that regulates the use of the certificate by the Owner as well as regulating the

relations between Owner and CA. The request for the certificate implies full and unconditional acceptance of the provisions contained in this Manual.

9.7.3. Major force

Azienda Zero cannot be held responsible for the non-execution of the obligations assumed pursuant to the provisions of this Manual if this non-execution is due to causes not attributable to Azienda Zero, such as - by way of example and not limited to - unforeseeable circumstances, malfunctions of absolutely unpredictable technical order and placed beyond any control, interventions of the authority, causes of force majeure, natural disasters, even corporate strikes - including those with subjects of which the parties avail themselves in carrying out the activities related to the service here described - and other causes attributable to third parties.

ANNEX A - Verification system for qualified electronic certificates

INDICATION OF THE SIGNATURE VERIFICATION SYSTEM

AZIENDA ZERO, in accordance with the provisions of art. 14 co.1 of the D.P.C.M. of February 22, 2013, provides and indicates to interested parties an application that allows the verification of qualified and digital electronic signature certificates affixed to electronic documents (according to CAdES, PAdES and XAdES standards).

In particular, the following online application is available for free, reachable at the address:

https://vol.uanataca.com/it

The aforementioned software specifically allows you to check:

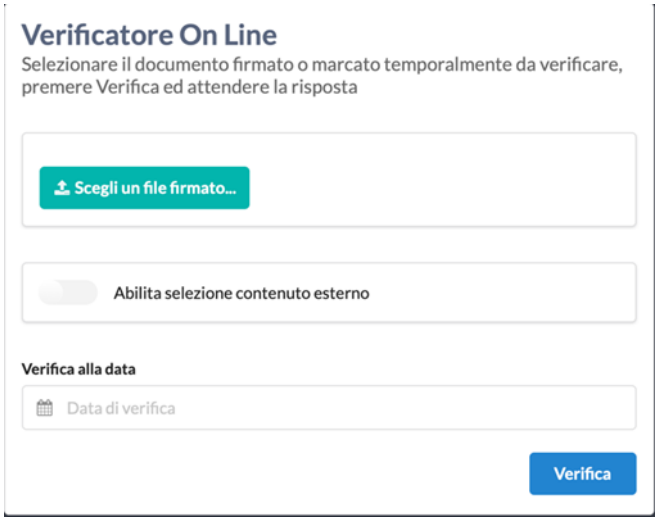
a) the identity of the signed document and the data of the signing party;

b) the authenticity and reliability of the certificate used to sign the document;

c) any states of suspension or revocation of the certificates used for signing;

OPERATING METHODS TO USE THE VERIFICATION APPLICATION

In order to verify the certificate of a qualified or digital signature according to the following methods, an internet connection is required. Once you reach the application web page at the link indicated above, the user will see the window in the following illustration:



- It will be sufficient, therefore, to select the "Choose a signed file" box and choose the file to be checked from the documents on the user's local computer;

- Once the file to be uploaded has been selected, the user must indicate the date on which the document was signed and finally click on the "Verify" button in order to verify its validity;
- At this point, the software will present the result of the verification by displaying a screen in which all the data necessary for the verification will be indicated.
- The user can also download the Verification Report, a document in PDF format (viewable via the free Adobe Reader or similar program), by clicking on the "PDF Report" button, which shows the outcome of the procedure verification.

The application, present at the address https://vol.uanataca.com/it, allows the user to carry out a verification on digital or qualified signature certificates whose result is fully compliant with the requirements of art. 14 co. 2 of the D.P.C.M. mentioned above.